James E. Cecchi
Lindsey H. Taylor
CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
(973) 994-1700

Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100

Counsel for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

MARK JOHNSTON, individually and on behalf of all others similarly situated, Plaintiff, v. QUEST DIAGNOSTICS, INC., and OPTUM360 LLC, Defendants.	Civil Action No.: **COMPLAINT and** **DEMAND FOR JURY TRIAL**

Plaintiff, Mark Johnston, individually and on behalf of all persons similarly situated, brings this class action Complaint against Defendants Quest Diagnostics Incorporated ("Quest") and Optum360 LLC ("Optum360") (collectively, "Defendants"), based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action on behalf of a nationwide class against Quest for its failure to secure and safeguard millions of patients' confidential information – including financial information, medical information, other personally identifiable information ("PII"), and/or other protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively "Personal Information") – and for failing to provide timely, accurate and adequate notice to Plaintiff and other Class Members that their Personal Information had been compromised.

2. Quest is one of the largest medical testing providers in the country. It collects private personal, medical, and financial information from its customers in providing its services. Optum360 is Quest's revenue cycle management provider. Retrieval-Masters Creditors Bureau Inc., d/b/a American Medical Collection Agency, Inc. ("AMCA") is Quest's billing collection vendor. As a part of the billing collection services, Quest and Optum360 share certain patient information with AMCA.

3. On June 3, 2019, Quest disclosed in a filing with the Securities and Exchange Commission (the "SEC") that Quest and Optum360 had been notified by AMCA on May 14, 2019 "about unauthorized activity on AMCA's web payment page" between August 1, 2018 and March 30, 2019.[1] Quest disclosed that information for 11.9 million of its patients "was contained on AMCA's affected system."[2] The information "included financial information (*e.g.*, credit card numbers and bank account information), medical information and other personal information (*e.g.*,

[1] Quest Diagnostics Form 8-K, filed June 3, 2019, available at https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm (last visited June 18, 2019).
[2] *Id.*

Social Security Numbers)[.]"[3] The cyber security event disclosed by Quest on June 3, 2019 is referred to hereinafter as the "Data Breach."

4. On its website, Quest states that AMCA has advised it will be sending letters to patients notifying them if their "social security number or financial information was involved in the incident."[4] Plaintiff Johnston received a notification letter from AMCA after having a laboratory test processed with Quest, which required the collection of his Personal Information.

5. Quest breached its duty to patients from across the country by sharing patient information with a third-party vendor that employed severely deficient data security practices. The security deficiencies were so significant that the intrusion remained undetected for nearly eight months even as patient information was being placed for sale on underground marketplaces known as the "dark web."

6. As set forth herein, the Data Breach was the inevitable result of Quest's inadequate approach to data security and its failure to protect its patients' Personal Information that it collected and disseminated to Optum360 and AMCA during the course of its business.

7. Plaintiff, on behalf of himself and similarly situated individuals, seeks to recover damages, equitable relief, and injunctive relief requiring Defendants to implement and maintain reasonable and industry-standard data security and data-sharing practices designed to prevent a reoccurrence of the Data Breach.

---

[3] *Id.*

[4] Quest Diagnostics, *AMCA Data Security Incident*, available at https://www.questdiagnostics.com/home/AMCA-data-breach-patients.html#q1-7 (last visited June 18, 2019).

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members. And, at least some members of the proposed Class have a different citizenship from Defendants. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because Defendant Quest resides in this District, transacts business in this District, and its principal place of business is located in this District. Accordingly, a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District. Venue is also proper under 28 U.S.C. § 1391(b)(3) because all Defendants are subject to personal jurisdiction in this District.

10. This Court has personal jurisdiction over Defendants because Defendants do business in and throughout the State of New Jersey, and the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues. Additionally, Defendant Quest's corporate headquarters are located within this District in Secaucus, New Jersey.

PARTIES

11. Plaintiff Mark Johnston is a resident and citizen of Orange, Ohio, whose Personal Information was compromised in the Data Breach described herein.

12. Defendant Optum360 LLP is a Delaware limited liability company with its principal place of business in Eden Prairie, Minnesota.

13. Defendant Quest Diagnostics is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

STATEMENT OF FACTS

A. The Data Breach

14. Quest is "the world's leading provider of diagnostic information services."[5] The patients it serves "comprise approximately one-third of the adult population of the United States annually, and approximately one-half of the adult population in the United States over a three-year period."[6] As part of its diagnostic information services business, Quest provides testing services "for the predisposition, diagnosis, treatment and monitoring of cancers and other diseases," routine, non-routine, or advanced clinical laboratory testing, and many other testing services.[7]

15. AMCA, according to its website, is "the leading Patient recovery agency" and is "one of the nation's top agencies managing over $1BN in annual receivables."[8] The AMCA has consistently received negative reviews from consumers, including receiving an "F" rating from the Better Business Bureau.[9] The Consumer Financial Protection Bureau ("CFPB") has received nearly 700 consumer complaints against the AMCA since 2013.[10]

16. On June 3, 2019, Quest publicly announced the following in a filing with the SEC:

> On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest Diagnostics Incorporated ("Quest Diagnostics") and Optum360 LLC, Quest Diagnostics' revenue cycle management provider, of potential unauthorized activity on AMCA's web payment page. Quest Diagnostics

---

[5] Quest Diagnostics 2018 Form 10-K, at 1, available at https://www.sec.gov/Archives/edgar/data/1022079/000102207919000030/dgx1231201810-k.htm (last visited June 18, 2019).
[6] *Id.* at 2.
[7] *Id.* at 10-11.
[8] AMCA, *About Us*, available at http://amcaonline.com/ (last visited June 18, 2019).
[9] Better Business Bureau, *American Medical Collection Agency*, available at https://www.bbb.org/us/md/baltimore/profile/collections-agencies/american-medical-collection-bureau-0011-90192010 (last visited June 18, 2019).
[10] CFPB Consumer Complaint Database, *Retrieval Masters*, available at https://www.consumerfinance.gov/data-research/consumer-complaints/search/?from=0&searchField=all&searchText=Retrieval%20Masters&size=25&sort=created_date_desc (last visited June 18, 2019).

> and Optum360 promptly sought information from AMCA about the incident, including what, if any, information was subject to unauthorized access.
>
> Although Quest Diagnostics and Optum360 have not yet received detailed or complete information from AMCA about the incident, AMCA has informed Quest Diagnostics and Optum360 that:
>
> - between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself;
> - the information on AMCA's affected system included financial information (*e.g.*, credit card numbers and bank account information), medical information and other personal information (*e.g.*, Social Security Numbers);
> - as of May 31, 2019, AMCA believes that the number of Quest Diagnostics patients whose information was contained on AMCA's affected system was approximately 11.9 million people; and
> - AMCA has been in contact with law enforcement regarding the incident.[11]

17. Although Quest reported that it had only learned of the Data Breach from AMCA on May 14, 2019, the breach was actually discovered at least three months prior to Quest's SEC filing. At the end of February 2019, Gemini Advisory, a New York-based company that works with financial institutions to monitor the sale of consumer information on underground markets, identified a large number of compromised AMCA patient information for sale on the dark web.[12] As reported on May 10, 2019 by DataBreaches.net:

> On February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark web marketplaces. Almost 15% of these records included additional personally identifiable information (PII), such as dates of birth (DOBs), Social Security numbers (SSNs), and physical addresses. A thorough analysis indicated that the information was likely stolen from the online portal of the American Medical Collection Agency (AMCA), one of the largest recovery agencies for patient collections. Several financial institutions also

[11] Quest Diagnostics Form 8-K, filed June 3, 2019, available at https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm (last visited June 18, 2019).

[12] Gemini Advisory, *AMCA Breach May be Largest Medical Breach in 2019* (June 4, 2019), available at https://geminiadvisory.io/amca-largest-medical-breach/ (last visited June 18, 2019).

collaboratively confirmed the connection between the compromised payment card data and the breach at AMCA.[13]

18. Gemini's additional research revealed AMCA's exposure window had lasted for at least seven months beginning in September 2018.[14]

19. On March 1, 2019, Gemini Advisory attempted to notify AMCA of the data exposure but received no response. Gemini Advisory then contacted federal law enforcement who reportedly followed-up with AMCA.[15]

20. In its notice to patients affected by the breach, AMCA claims it learned of the unauthorized access on March 20, 2019. Yet, Quest failed to take any steps to notify patients whose information was affected until June 3, 2019, at which point Quest only did so through an SEC filing.

21. Subsequent to Quest's SEC filing, AMCA began sending out notices to those affected by the data breach. Quest stated on its website that it had "been advised by AMCA that if your social security number or financial information was involved in the incident, you will be notified by letter from AMCA[.]"[16]

22. On June 17, 2019, AMCA filed for Chapter 11 bankruptcy in the Southern District of New York stating an intention to liquidate. The bankruptcy filings describe the types of personal

---

[13] Databreaches.net, *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory* (posted May 10, 2019), available at https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/ (last visited June 18, 2019).

[14] *Id.*

[15] *Id.*

[16] Quest Diagnostics, *AMCA Data Security Incident*, available at https://www.questdiagnostics.com/home/AMCA-data-breach-patients.html (last visited June 18, 2019).

information maintained by AMCA as well as additional specifics regarding the Data Breach. An affidavit submitted by Russell H. Fuchs, the Chief Executive Officer of AMCA, stated as follows:

> [AMCA] by its very nature, requires it to collect and maintain data transmitted to it by its clients that includes personally identifiable information about third-party debtors that could include names, home addresses, social security numbers, bank account information for consumers choosing to pay online by check and, for consumers choosing to pay their outstanding balances by credit card, credit card information. In the case of the AMCA business, that information might also include dates of birth and certain medical information related to any laboratory tests for which payment is sought. In all, at any given time, [AMCA] would have held tens of millions of individual points of data regarding millions of individual persons, none of which could be handled without a robust IT system.
>
> [AMCA]'s original IT architecture was built around an IBM mainframe-based system that ran on COBOL4 and served the [AMCA]'s purposes well for many years. However, with ever-increasing market demands for enhanced interconnectivity between the [AMCA]'s and its clients' systems, as well as for web-based interaction with both the [AMCA]'s clients and its clients' consumer and patient-debtors, it was clear that continued reliance on the [AMCA]'s internet-unconnected mainframe system would not be tenable in the long term.
>
> Accordingly, in 2015, after several years of internal planning and development, the [AMCA] began to transition to a proprietary, server-based, network-connected system. [AMCA] invested over a million dollars in the new system, employing outside IT consultants to ensure that the system would reflect current technological standards, including, importantly, appropriate data security protocols.[17]

23. Despite touting its investment in data security, AMCA acknowledged that it "first learned that there might be a problem" when it received a series of common point of purchase notifications that "suggested that a disproportionate number of credit cards that at some point had interacted with the [AMCA's] web portal were later associated with fraudulent charges."[18]

24. In response, AMCA "shut down its web portal to prevent any further compromises of customer data, and engaged outside consultants who were able to confirm that, in fact, [AMCA]'s servers … had been hacked as early as August, 2018." AMCA went on to explain that

[17] *In re Retrieval-Masters Creditors Bureau, Inc*., No. 7:19-bk-23185, Dkt. No. 2 (Bankr. S.D.N.Y. Jun 17, 2019).
[18] *Id*.

"the breach required [AMCA] to hire IT professionals and consultants from three different firms, to identify the source of the breach, diagnose its cause, and implement appropriate solutions. To date, these expenses alone cost approximately $400,000, and have effectively shut down outside entry into [AMCA]'s IT network by severely restricting access via the employment of individual authentication mechanisms, VPN access, or specifically vetted 'whitelists' of pre-approved IP's."[19]

25. AMCA stated that the costs of providing notice to affected individuals, coupled with the loss of its largest clients LabCorp and Quest, required it to reduce its workforce from 113 employees at year-end 2018 to just 25 employees as of June 17, 2019. As a result, AMCA stated it is "no longer is optimistic that it will be able to rehabilitate its business." [20]

26. Quest had a non-delegable duty to ensure that its systems and those of its third-party vendors, including AMCA, were sufficient to adequately secure patient information. This was especially true after AMCA transitioned to a "network-connected" system that included "enhanced interconnectivity" and "web-based interaction" between its systems and those of its clients such as Quest and Optum360.

27. By failing to adequately monitor and audit the data security systems of their vendors and business associates, Quest put patient information at severe risk. Quest has not indicated how or even whether it will notify all affected 11.9 million of its customers who are breach victims, stating only that it is "working to ensure that affected Quest patients receive notice of the AMCA incident consistent with state and federal law."[21]

---

[19] *Id*.
[20] *Id*.
[21] Quest Diagnostics, *AMCA Data Security Incident*, available at https://www.questdiagnostics.com/home/AMCA-data-breach-patients.html (last visited June 18, 2019).

B. Plaintiff's Notification of the Data Breach

28. Plaintiff Johnston had a laboratory test processed with Quest, which required the collection of Plaintiff Johnston's Personal Information. Upon information and belief, Quest then provided Plaintiff's Personal Information to AMCA.

29. Plaintiff Johnston received a "Notice of Data Breach" dated June 4, 2019 from AMCA. The notice stated that on March 20, 2019 the AMCA had "received notice of a possible security compromise" and that it had "recently learned, after an external forensics review, that an unauthorized user had access to our system between August 1, 2018 and March 30, 2019, and cannot rule out the possibility that the personal information on our system was at risk during the attack."

30. The notice further stated that the "information on our system that was compromised may have included your: first and last name, Social Security Number, name of lab or medical service provider, data of medical service, referring doctor, certain other medical information, but not test results."

31. AMCA stated in the notice that it had "arranged to provide [Plaintiff] with 24 months of complimentary credit monitoring and identity theft mitigation services" but also recommended that Plaintiff take numerous actions on his own. It recommended that Plaintiff: (1) "remain vigilant for fraud and identity theft by reviewing and monitoring [his] account statements and credit reports closely;" (2) contact the FTC or various attorneys general if Plaintiff believes he was the "victim of identity theft or ha[s] reason to believe [his] personal information has been misused;" (3) contact "any one of the three credit bureaus … and place a fraud alert on [his] credit report file;" and (4) place a "credit freeze, also known as a security freeze, on [his] credit file[.]"

32. Since receiving the breach notification letter, Plaintiff Johnston now engages in frequent monitoring of his financial and credit accounts and has spent time and effort attempting to protect himself against identity theft and fraud.

C. Defendants' Privacy Practices

33. Defendants had obligations, arising from promises made to patients like Plaintiff and Class Members, and based on industry standards, to keep the compromised Personal Information confidential and to protect it from unauthorized disclosure.

34. Quest had obligations under HIPAA to keep the compromised Personal Information confidential and prevent unauthorized disclosures. Quest is subject to HIPAA's regulations,[22] which include the Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

35. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be sued to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

36. Optum360 also had obligations under HIPAA. The Health Information Technology for Economic and Clinical Health Act ("HITECH") imposes a number of HIPAA's Privacy Rule

[22] *See* Quest Diagnostics 2018 Form 10-K, at 26, *available at* https://www.sec.gov/Archives/edgar/data/1022079/000102207919000030/dgx1231201810-k.htm (last visited June 18, 2019).

requirements and a majority of HIPAA's Security Rule provisions directly on business associates of covered entities.

37. Plaintiff and Class Members provided their Personal Information to Quest with the understanding that Quest and any business associates to whom it provided the information, such as AMCA and Optum360, would comply with their obligations to adopt appropriate data security measures to keep the information confidential and secure.

38. In its 2018 Form 10-K, Quest represented that it "strive[s] to conduct [its] business in compliance with all applicable laws and regulations," including HIPAA, and that it has a "long-standing and well-established compliance program," which includes "detailed policies and procedures and training programs intended to ensure the implementation and observance of all applicable laws and regulations […] and Company policies." It also represents that it "conduct[s] in-depth reviews of procedures and facilities to assure regulatory compliance throughout [its] operations."[23]

39. In addition to its representations in its Form 10-K, Quest maintains a Notice of Privacy Practices on its website, which states as follows:

> Quest Diagnostics is required by law to maintain the privacy of your PHI. We are also required to provide you with this Notice of our legal duties and privacy practices upon request. It describes our legal duties, privacy practices and your patient rights as determined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). We are required to follow the terms of this Notice currently in effect. We are required to notify affected individuals in the event of a breach involving unsecured protected health information. PHI is stored electronically and is subject to electronic disclosure. This Notice does not apply to non-diagnostic services that we perform such as certain drugs of abuse testing services and clinical trials testing services.[24]

---

[23] *Id.* at 26.

[24] Quest Diagnostics, *Notice of Privacy Information*, available at https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html (last visited June 18, 2019).

40. Quest also addresses its practice of sharing patient information with business associates, reassuring that its associates are "required to maintain the privacy and security of [patients'] PHI":

> We may provide your PHI to other companies or individuals that need the information to provide services to us. These other entities, known as 'business associates,' are required to maintain the privacy and security of PHI. For example, we may provide information to companies that assist us with billing of our services. We may also use an outside collection agency to obtain payment when necessary.[25]

41. Despite these representations, Quest's security failures demonstrate that it failed to comply with their duties under HIPAA and its own Privacy Practices. Indeed, Quest and Optum360 failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protect Plaintiff's and the Class Members' Personal Information;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. 164.312(a)(1);

e. Implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

[25] *Id.*

f. Implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

42. Quest failed to comply with its duties under the law and its own Privacy Policy despite the fact that it was on high alert to the potential of data security breaches.

43. In fact, Quest previously suffered a data breach in November 2016 when an unauthorized third party accessed Quest's patient portal known as "MyQuest" and obtained the PHI of approximately 34,000 patients.[26]

44. Further, Defendants were also on notice that healthcare companies are a prime target for cyberattacks. For example, in August 2014, after a cyber-attack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that "[t]he FBI has observed

[26] Quest Diagnostics, *Quest Diagnostics Provides Notice of Data Security Incident* (Dec. 12, 2016), available at http://ir.questdiagnostics.com/node/13111/pdf (last visited June 18, 2019).

malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[27] Indeed, in recent years, there have been numerous high-profile attacks against companies within the healthcare industry, such as the 2015 data breach involving health insurer Anthem, Inc. in which cyberattackers stole the personal information of approximately 80 million Americans.[28]

45. Defendants were also generally on notice of the threat of cyberattacks due to prior, high-profile security breaches at retail chains such as Home Depot, Target, and Neiman Marcus, as well as in other industries, such as the recent high-profile breaches involving Equifax and Marriott.

D. The Data Breach Caused Harm and Will Result in Additional Fraud

46. The ramifications of Defendants' failure to keep Plaintiff's and Class Members' data secure are severe. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." *Id*.

47. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[29]

---

[27] Jim Finkle, *FBI warns healthcare firms that they are targeted by hackers,* REUTERS (Aug. 2014, 4:32 PM), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited June 18, 2019).

[28] Bank Info Security, *A New In-Depth Analysis of Anthem Breach* (Jan. 10, 2017), available at https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627 (last visited June 18, 2019).

[29] Federal Trade Commission, *Warning Signs of Identity Theft* (May 2015), available at https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited June 18, 2019).

48. Identity thieves can use personal information, such as that of Plaintiff and Class Members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

49. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[30]

50. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

---

[30] Federal Trade Commission, *Combating Identity Theft A Strategic Plan* (April 2007), available at https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited June 18, 2019).

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[31]

51. Personal Information such as that stolen in Data Breach is highly coveted by, and a frequent target of, hackers because thieves can use the credit card information to create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; thieves can reproduce stolen debit cards and use them to withdraw cash from ATMs; use the victim's Personal Information to commit immigration fraud, obtain a driver's license or identification card in the victim's name but with another's picture, use the victim's information to obtain government benefits, file a fraudulent tax return using the victim's information to obtain a fraudulent refund; get medical services using consumers' stolen information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

52. The lucrative market for this information is evidenced by the fact that information stolen in the Data Breach has already been placed for sale on underground markets. In fact, AMCA only discovered the breach after a third-party watchdog observed fraudulent charges on a

[31] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), available at http://www.ssa.gov/pubs/10064.html (last visited June 18, 2019).

disproportionate number of credit cards that were linked to AMCA. The fact that this information is already being sold and used to commit identity theft and fraud means Plaintiff and all Class Members are already at a serious and imminent risk of harm.

53. Further, without detailed, prompt disclosure by Quest to its patients who have been impacted, affected individuals, including Plaintiff and Class Members, have been left exposed, unknowingly and unwittingly, for months to continued misuse and ongoing risk of misuse of their Personal Information without being able to take necessary precautions to prevent imminent harm.

54. And even those individuals who are reimbursed for a financial loss due to fraud are not made whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[32]

55. There may also be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[33]

[32] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Sept. 2015) available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited June 18, 2019).

[33] U.S. Government Accountability Office, *Report to Congressional Requesters* (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited June 18, 2019).

56. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records and will continue to spend time, effort, and money attempting to protect themselves from ongoing identity theft and fraud.

E. Plaintiff and Class Members Suffered Damages

57. The Personal Information of Plaintiff and Class Members is private and sensitive in nature and was left inadequately protected by Defendants.

58. The Data Breach was a direct and proximate result of Quest's failure to adequately monitor and audit the data security systems of its vendors, including Optum360 and AMCA, and its failure to properly safeguard and protect Plaintiff's and Class Members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including its failure to establish, implement, and ensure appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Personal Information to protect against reasonably foreseeable threats to the security or integrity of such information.

59. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach. Indeed, as warned by Maryland's Attorney General in the aftermath Data Breach: "Massive data breaches like the one experienced by the AMCA are extremely alarming, especially considering the likelihood that personal, financial, and medical information may now be in the hands of thieves and scammers. I strongly urge consumers to take steps to ensure that their information and personal identity is

protected."[34] He then provided a list of recommended actions for victims to take, including: (1) obtaining a free credit report, (2) putting a fraud alert on your credit file, (3) considering placing a security freeze on your credit file, (4) taking advantage of any free services being offered as part of the breach, and (5) using two-factor authentication for online accounts wherever available.

60. Further, as discussed above, AMCA itself recommended that impacted individuals take precautionary measures, such as closely monitoring account statements and credit reports, contacting the FTC or various attorneys general if they believe they are a victim of identity theft, and placing fraud alerts or security freezes on accounts.

61. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Personal Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation.

62. Defendants continue to hold patients' Personal Information, including the Plaintiff's and Class Members' Personal Information, and, therefore, Plaintiff and the Class have an undeniable interest in ensuring that their Personal Information is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ALLEGATIONS

63. Plaintiff seeks relief on behalf of himself and as a representative of all others who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a nationwide class defined as follows:

[34] Washington's Top News, *Maryland AG warns residents of massive medical data breach* (June 14, 2019), available at https://wtop.com/maryland/2019/06/maryland-ag-warns-residents-of-massive-medical-data-breach/ (last visited June 18, 2019).

> All persons in the United States whose Personal Information was compromised as a result of the breach announced by Quest Diagnostics on or around June 3, 2019 (the "Class").

64. Excluded from the above Class are Defendants and any of their affiliates, parents or subsidiaries; all employees of Defendants; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

65. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

66. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

67. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, the proposed Class includes potentially thousands or millions of individuals whose Personal Information was compromised in the Data Breach. Class members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

68. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Defendants had a duty to protect Personal Information;

b. Whether Defendants knew or should have known of the susceptibility of AMCA's systems to a data breach;

c. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

d. Whether Defendants' security measures to protect its systems were reasonable in light known legal requirements;

e. Whether Defendants were negligent in failing to adequately monitor and audit the data security systems of their vendors and business associates;

f. Whether Quest's efforts (or lack thereof) to ensure the security of patients' Personal Information provided to business associates were reasonable in light of known legal requirements;

g. Whether Defendants' conduct constituted unfair or deceptive trade practices;

h. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of AMCA's systems and/or the loss of the Personal Information of Plaintiff and Class Members;

i. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect their Personal Information; and,

j. Whether Plaintiff and Class members are entitled to relief.

69. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class Members. Plaintiff's Personal Information was in Defendants' possession at the time of the Data Breach and was compromised as a result of the

Data Breach. Plaintiff's damages and injuries are akin to other Class Members and Plaintiff seeks relief consistent with the relief of the Class.

70. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

71. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

72. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds

generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

73. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants' owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendants failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiff and the Class members;

c. Whether Defendants failed to adequately monitor and audit the data security systems of their vendors and business associates;

d. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class against Defendants)

74. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

75. Quest required Plaintiffs and Class Members to submit Personal Information to obtain diagnostic and medical services, which Quest provided to Optum360 and AMCA for billing purposes. Defendants collected and stored the data for commercial gain.

76. Quest had a non-delegable duty to ensure that any associated entities with whom it shared patient information maintained adequate and commercially-reasonable data security practices to ensure the protection of patients' Personal Information.

77. Defendants owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' Personal Information within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

78. Defendants owed a duty of care to Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the Personal Information.

79. Defendants' duty to use reasonable care in protecting Personal Information arose as a result of the common law and the statutes and regulations, such as the HIPAA regulations described above, as well as their own promises regarding privacy and data security to their patients.

80. Defendants knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its vendor's system, and the importance of adequate security. Quest specifically knew about the risks inherent in collecting and storing Personal Information given its experience with a recent cyber-attack in November 2016 and its acknowledgment that Quest's "business associates" are "required to maintain the privacy and security of [patients'] PHI."

81. Defendants breached their common law, statutory, and other duties – and thus were negligent – by failing to use reasonable measures to protect patients' Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

82. Defendants breached their duties to Plaintiff and Class Members in numerous ways, including by:

a. failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' Personal Information;

b. failing to comply with industry standard data security standards during the period of the Data Breach;

c. failing to adequately monitor and audit the data security systems of their vendors and business associates;

d. failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

e. failing to adequately monitor, evaluate, and ensure the security of AMCA's network and systems;

f. failing to recognize in a timely manner that Plaintiff's and other Class Members' Personal Information had been compromised;

g. failing to timely and adequately disclose that Plaintiff's and Class members' Personal Information had been improperly acquired or accessed.

83. Plaintiff's and Class Members' Personal Information would not have been compromised but for Defendants' wrongful and negligent breach of their duties.

84. Defendants failure to take proper security measures to protect sensitive Personal Information of Plaintiff and Class Members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Personal Information of Plaintiff and Class Members.

85. It was also foreseeable that Defendants' failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and other Class Members.

86. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

87. As a direct and proximate cause of Defendants' conduct, Plaintiff and the Class suffered damages and will suffer damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiff and Class Members; damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take years to discover and detect.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class against Defendants)

88. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

89. HIPAA requires Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

90. HIPAA further requires Defendants to disclose the unauthorized access and theft of the Personal Information to Plaintiff and the Class "without unreasonable delay" so that Plaintiff

and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, .406, .410.

91. Defendants violated HIPAA by failing to reasonably protect Plaintiff's and Class Members' Personal Information, as described herein.

92. Defendants' violations of HIPAA constitute negligence *per se*.

93. Plaintiff and Class Members are within the class of persons that HIPAA was intended to protect.

94. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

95. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

96. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

97. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach at companies as large as Quest, including, specifically, the immense damages that would result to Plaintiff and Class Members.

98. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

99. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

100. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

101. As a direct and proximate result of Defendants' negligence *per se* under HIPAA and the FTC Act, Plaintiff and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class against Defendants)

102. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

103. Plaintiff and Class Members were required to provide their Personal Information, including names, addresses, Social Security numbers, financial information, and other personal information, to Quest in order to complete medical and diagnostic tests.

104. When Plaintiffs and Class Members paid money and provided their Personal Information to Quest in exchange for services, they entered into implied contracts with Quest and its business associate, Optum360, pursuant to which Defendants agreed to safeguard and protect such information and to timely and adequately notify them if their data had been breached and compromised.

105. Plaintiff and the Class Members would not have provided and entrusted their Personal Information to Defendants in the absence of the implied contract to keep the information secure.

106. Plaintiff and the Class Members fully performed their obligations under the implied contract with Defendants whereas Defendants did not.

107. Defendants breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Personal Information, which was compromised as a result of the Data Breach.

108. As a direct and proximate result of Defendants' breach of its implied contacts with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their Personal Information is used; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Personal Information in its continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class against Defendants)

109. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

110. Plaintiff and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Defendants and which was ultimately stolen in the Data Breach.

111. Defendants benefited by Plaintiff and Class Members' conferring upon them their Personal Information, which Defendants retain and use for business purposes and profit.

112. Plaintiff and Class Members also conferred a direct monetary benefit on Defendants. Specifically, they purchased medical services from Defendants and, in doing so, provided Defendants with their Personal Information. The amounts paid by Plaintiff and Class Members were used, in part, to pay for Defendants' costs associated with keeping the Personal Information private and secure.

113. Plaintiff's and the Class Members' Personal Information was private and confidential and its value depended upon Defendants' maintaining the privacy and confidentiality of that personal information.

114. But for Defendants' commitment to maintain the confidentiality and security of their Personal Information, Plaintiff and the Class Members would not have provided the information to Defendants.

115. As a result of the wrongful conduct alleged herein, Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members. Among other things, Defendants continue to benefit and profit from the use of Plaintiff's and the Class Members'

Personal Information, while its value to Plaintiff and Class Members has been diminished and its exposure has caused Plaintiff and Class Members' harm.

116. Under the doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits they received, and are still receiving, from Plaintiff and Class Members.

117. Equity and good conscience require restitution by the Defendants in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including, specifically, the value to Defendants of the Personal Information that was stolen in the Defendants' Data Breach and the resulting profits Defendants received and are receiving from the use of that information. Further, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class against Defendants)

118. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

119. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Defendants to provide adequate security for the Personal Information it collected from them. As previously alleged, Defendants owe duties of care to Plaintiff and Class Members that require it to adequately secure Personal Information.

120. Defendants still possess Personal Information pertaining to Plaintiff and Class Members.

121. Defendants have made no announcement or notification that they have remedied the vulnerabilities in their practices and policies regarding ensuring the data security of patients' Personal Information.

122. Accordingly, Defendants have not satisfied their implied contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendants' lax approach towards data security has become public, the Personal Information in their possession and in their vendors' possession is more vulnerable than it was prior to announcement of the Data Breach.

123. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide data security measures to Plaintiff and Class Members.

124. Plaintiff, therefore, seeks a declaration that (a) Defendants' existing data security measures do not comply with its obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Modifying their practices and policies to ensure the business associates to which they provide patients' Personal Information engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on their systems on a periodic basis, and ordering vendors to promptly correct any problems or issues detected by such third-party security auditors;

b. Modifying their practices and policies to ensure the business associates to which they provide patients' Personal Information engage third-party security auditors and internal personnel to run automated security monitoring;

c. Modifying their practices and policies to ensure the business associates to which they provide patients' Personal Information audit, test, and train security personnel regarding any new or modified procedures;

d. Modifying their practices and policies to ensure the business associates to which they provide patients' Personal Information segment Personal Information by, among other things, creating firewalls and access controls so that if one area of a system is compromised, hackers cannot gain access to other portions of the systems;

e. Modifying their practices and policies to ensure only Personal Information necessary for provision of services is provided to business associates;

f. Modifying their practices and policies to ensure Personal Information not necessary for the provision of services is purged, deleted, and destroyed, and to ensure its business associates likewise purge, delete, and destroy such Personal Information;

g. Conducting regular security checks of the business associates to which it provides patients' Personal Information;

h. Routinely and continually conduct internal training and education to inform internal security personnel how to monitor the data security of business associates to whom patients' Personal Information is provided; and

i. Educating its patients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendants' patients must take to protect themselves.

COUNT VI
NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. § 56:8-1, *et. seq.*
(On Behalf of Plaintiff and the Class against Defendant Quest)

125. Plaintiff restates and re-alleges the preceding paragraphs as if fully set forth herein.

126. Quest sells "merchandise," as meant by N.J.S.A. § 56:8-1, by offering health benefits services to the public.

127. Quest, operating in New Jersey, engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of health benefits services in violation of N.J.S.A. § 56:8-2, including but not limited to the following:

a. Quest misrepresented material facts, pertaining to the sale of health benefits services, to the Plaintiff and Class Members by representing that they would maintain adequate data security practices and procedures to safeguard Plaintiff's and Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. Quest misrepresented material facts, pertaining to the sale of health benefits services, to the Plaintiff and Class Members by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' Personal Information;

c. Quest knowingly omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and Class Members' Personal Information with the intent that Plaintiff and Class Members rely on the omission, suppression, and concealment;

d. Quest engaged in unconscionable and deceptive acts and practices with respect to the sale of health benefit services by failing to adequately monitor and audit the data security systems of its vendors and business associates and failing to maintain the privacy and security of Plaintiff's and Class Members in violation of duties imposed by and public policies reflected in the FTC Act and HIPAA;

e. Quest engaged in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiff and Class Members in a timely and accurate manner violation of N.J.S.A. § 56:8-163.

128. The above unlawful and deceptive acts and practices by Quest were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

129. Quest knew or should have known that their data security practices were inadequate to safeguard Plaintiff's and Class Members' Personal Information and that the risk of a data breach was highly likely. Quest's actions in engaging in the above-listed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

130. As a direct and proximate result of Quest's unconscionable and deceptive acts and practices, Plaintiff and Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

131. Plaintiff and Class Members seek relief under N.J.S.A. § 56:8-19, including but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in his favor and against Defendants as follows:

a. For an Order certifying the Class, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

b. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class members;

c. For equitable relief compelling Defendants to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class Members the type of Personal Information compromised;

d. For an award of damages, including nominal damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

CARELLA, BYRNE, CECCHI
OLSTEIN, BRODY & AGNELLO
Attorneys for Plaintiff

By: /s/James E. Cecchi
JAMES E. CECCHI

Dated: June 18, 2019

Norman E. Siegel
Barrett J. Vahle

J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel: (816) 714-7100
Fax: (816) 714-7101
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com

Counsel for Plaintiff and Proposed Class